AMENDMENTS TO THE DRAWINGS

The attached "Replacement Sheet" of drawings includes changes to Figure 1. The attached "Replacement Sheet," which includes Figure 1, replaces the original sheets including Figure 1.

Attachment: Replacement Sheet

REMARKS

Reconsideration of the present application is requested. Claims 1, 8, 22 and 31, paragraph [0020] and FIG. 1 have been amended. Support for amendments made to claims 1, 8, 22 and 31 may be found, for example, in paragraphs [0016], [0019], [0021] and [0023] of Applicants' Specification.

ENTRY OF AMENDMENT AFTER FINAL IS REQUESTED

Entry of this Amendment after Final is requested in that the amendments made herein do not raise new issues requiring further consideration and/or search. The amendments made herein only further clarify features previously set forth. Entry of this Amendment after Final is respectfully requested.

INFORMATION DISCLOSURE STATEMENT

The Examiner has considered the Information Disclosure Statement filed April 9, 2007.

PRIORITY

The Examiner acknowledges Applicants' claim for foreign priority under 35 U.S.C. § 119.

SPECIFICATION

The Examiner objects to the July 6, 2007 Amendment because the changes to paragraph [0020] allegedly introduce new matter. Although Applicants do not necessarily agree, paragraph [0020] has been revised taking

into account the Examiner's comments. Withdrawal of this objection is requested.

DRAWINGS

The Examiner objects to the drawings under 37 C.F.R. § 1.83(a) because the drawings allegedly do not show assigning a data key to a user. Moreover, the Examiner is apparently unable to find any support in the original disclosure for step 13 in FIG.1. Although Applicants do not necessarily agree with the Examiner's objections, Applicants have amended the drawings, the specification and the claims taking into account the Examiner's comments. As will be discussed in more detail below, the claims are fully supported by the specification. Withdrawal of this objection is requested.

REJECTION UNDER 35 U.S.C. § 112

Beginning on page 5 of the Office Action, the Examiner rejects claims 1-32 under 35 U.S.C. § 112, first paragraph, as allegedly failing to comply with the written description requirement. Particularly, the Examiner states in part:

> ...the Applicant added the new claim limitation of "assigning a data key to the user". The examiner respectfully and carefully reviewed the Applicant's original disclosure and did not find support in the original disclosure. In par. [0011], the Applicant discloses "...people...who have joint use of encrypted data not being assigned user specific data key for accessing the data.... The data key is automatically assigned but is not communicated to the user, i.e. the users receive no knowledge of the actual nature of the data key. Accordingly, they neither need to remember the data key nor are they able to communicate it....". Additionally, in par. [0012], the Applicant discloses "...instead, they are simply no longer assigned a valid data key if they attempt to access data".

The Examiner then concludes that, "it is very clear that both the new claim limitations and Applicants' argument on pp. 12-14 are contradicted with Applicants' original disclosure." Applicants disagree.

According to paragraph [0010], in example embodiments each user of jointly used encrypted data is identified on the basis of his association with a group. In doing so, users who jointly use the encrypted data are assigned a common user group data key on the basis of their association with a user group. All members of the user group may utilize the user group data key to encrypt and decrypt data intended for joint use.

To suppress significant security problems associated with conventional key systems, the user group data key is automatically assigned, but not communicated to the users, and thus, users receive no knowledge of the actual nature of the data key.

From the above discussion, one can appreciate that users having joint use of encrypted data are assigned a common user group data key on the basis of their association with a user group. While not assigned user specific data keys, users are still assigned a data key, albeit a group data key based on their association with a user group.

Based on the above, Applicants' Specification fully supports, but does not contradict, the claims. Withdrawal of this rejection is requested.

PRIOR ART REJECTIONS

Rejection under 35 U.S.C. § 103

The Examiner rejects claims 1-32 under 35 U.S.C. § 103(a) as allegedly unpatentable over U.S. Patent No. 6,031,910 ("*Deindl*"). This rejection is respectfully traversed.

Claim 1 is directed to a method in which a security check is performed to ascertain an identity of a user, and the user is associated with a user group including a plurality of users such that a data key is assigned to the user based on the user group with which the user is associated. The data key is unviewable by the user and is for at least one of encrypting and decrypting data. The same data key is assignable to the plurality of users.

Deindl discloses a system and method for secure storage and transmission of protectable information using a patient card. Abstract. The system of *Deindl* includes two separate cards, a user card 310 and patient card 350. *Deindl* at 4:39-4:41. The user card 310 is carried by a doctor or other health professional (*Id.* at 4:53-4:54) and includes a set of group data keys programmed by a system operator. The set of group keys legitimize the doctor carrying the card 310 as an authorized specialist in a particular area. *Id.* at 4:54-4:55, 7:58-7:62.

The patient card 350 is carried by a patient and includes patient data. *Deindl* at 4:48-4:52. Each patient card 350 contains its own encryption/decryption function *Id.* at 6:15-6:20.

In one embodiment, if a doctor requires access to protected data on the patient card 350, each of the cards 310 and 350 are inserted into card reader portions of the system. The information regarding the doctor's group is read from user card 310 and stored on that patient card 350. The system reads a file containing medical data on the patient from the patient card 350 and separates the data into a data header 110 and a data record 120. The header 110 including decryption information is sent to the patient card 350.

The patient card 350 verifies that the group information from the user card 310 matches the group information from the header 110. If authorized, the system extracts an encrypted key (for decrypting the data record 120) from the header 110 and sends the key to the patient card 350. The patient card 350 decrypts the key and sends the decrypted key back to the system for decrypting the data record 120. *See, generally, Deindl* at 5:1-5:23.

In contrast to claim 1, *Deindl* fails to teach or fairly suggest, "*associating the user with a user group including a plurality of users such that a data key is assigned to the user based on the user group with which the user is associated,*" In *Deindl*, the set of group keys are programmed on the user card 310 by a system operator. The set of group keys are assigned to the user card 310, not the user.

Notwithstanding the above, *Deindl*'s the set of group keys on the user card 310 are not for encrypting or decrypting data. The group keys on the user card 310 merely represent the group to which the user belongs. As discussed in detail above, all encryption/decryption keys are stored on the patient card

350 (*Deindl* at 6:20 – 6:43), which are completely separate from the set of group keys stored on the user card 310. Further, the cryptographic keys on the patient card 350 are not assigned to a user, "based on the user group with which the user is associated," as required by claim 1. Consequently, *Deindl* fails to teach or fairly suggest at least, "*associating the user with a user group including a plurality of users such that a data key is assigned to the user based on the user group with which the user is associated*," "*the data key being for at least one of encrypting and decrypting data*," as required by claim 1.

For at least the foregoing reasons claim 1 is patentable over *Deindl*.

Claims 8, 22 and 31 are patentable over *Deindl* for at least reasons somewhat similar to those set forth above with regard to claim 1.

Claims 2-7, 9-21, 23-30 and 32 are patentable at least by virtue of their dependency from claims 1, 8, 22 or 31.

CONCLUSION

Accordingly, in view of the above amendments and remarks, reconsideration of the objections and rejections and allowance of each of claims 1-32 in connection with the present application is earnestly solicited.

If the Examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to telephone Andrew M. Waxman, Reg. No. 56,007, at the number of the undersigned listed below.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies to charge payment or credit any overpayment to Deposit

Account No. 08-0750 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY & PIERCE, PLC

By #56,007
Donald J. Daley
Reg. No. 34,313

DJD/AMW:krm

P.O. Box 8910
Reston, VA 20195
(703) 668-8000